2131
#7/B
12-31-02

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Teow HIn NGAIR

Appln. No.: 09/831,491

Confirmation No.: 5659

Filed: May 09, 2001

Docket No: Q64409

Group Art Unit: 2131

Examiner: UNKNOWN

For: A METHOD OF ENCRYPTION AND APPARATUS THEREFOR

SECOND PRELIMINARY AMENDMENT

Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination, please further amend the above-identified application as follows:

IN THE CLAIMS:

Please cancel claims 10-12 without prejudice or disclaimer.

Please enter the following amended claims:

1. (Amended) A method of generating a private key signature in respect of user data using a token, the token having stored therein a private key and a symmetric key, said method comprising the steps of

a.   providing the user data or a representation thereof as an input to a symmetric key operation supported by the token,

b.   retrieving the output of the symmetric key operation as the token signature; and

c.   combining the token signature with the user data or representation to generate the token bound output data; and

d.   providing the output data as an input parameter to a private key signature generation operation, to form a private key signature for the user data.